



CVE-1999-1558

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-1999-1558
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	1998-07-16 04:00:00 UTC
Updated	2008-09-05 20:19:00 UTC
Description	Vulnerability in loginout in Digital OpenVMS 7.1 and earlier allows unauthorized access when external authentication is ena

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digital	Digital Openvms	7.1	All	All	All
Application	Digital	Digital Openvms	7.1	All	All	All
Application	Digital	Digital Openvms Axp	7.1	All	All	All
Application	Digital	Digital Openvms Axp	7.1	All	All	All

References

Reference	Source
ISS X-Force Database: openvms-loginout-unauth-access (7151): OpenVMS LOGINOUT could allow unauthorized system access	XF
OpenVMS loginout Vulnerability	CIAC
OpenVMS loginout Vulnerability	BID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)